International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

Volume 2 Issue 1 January 2013

International Manuscript ID : ISSN22308849-V2I1M7-012013

COMPARISON OF VARIOUS WLAN SECURITIES

SHIKHA BANSAL, MANISH MAHAJAN
CGC, Landran, Punjab

Abstract
As Wireless Local Area Networks (WLANs) are rapidly deployed to expand the field of wireless products, the provision of authentication and privacy of the information transfer will be mandatory. WLANs are also playing much larger role in corporate network environments and are already very popular for home networking applications. This increase in accessibility has created large security holes for hackers and thieves to abuse, that is finally being addressed by stronger security protocols and these security protocols include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and 802.11i (WPA2).

These functions need to take into account the inherent limitations of the WLAN medium such as limited bandwidth, noisy wireless channel and limited computational power. Even when security measures are enabled in Wi-Fi devices, a weak encryption protocol such as WEP is usually used. In this article, we will examine the weaknesses of WEP and see how easy it is to crack the protocol. The lamentable inadequacy of WEP highlights the need for new security architecture in the form of the 802.11i standard, so we will also take a look at the new standard's WPA and WPA2 implementations along with their possible vulnerabilities and comparison of various WLAN securities.

Introduction

Wireless techniques have displayed significant development within the last few years in both house and corporate surroundings due in part to low price and increased components quality. This development has motivated new applications for Wi-Fi techniques which range from advanced factory stock techniques to Wi-Fi above (VoIP) phones. The ease of use and vast submission of these techniques has created a protection headache for house customers and system directors, which has become widely promoted in the media. The first version of the IEEE 802.11 standard supported a basic mechanism for protecting such networks named Wired Equivalent Privacy (WEP) [1]. WEP requires all clients and access points in the network to share up to four different secret symmetric keys, which is clearly not optimal for a larger installation where users change frequently. Most installations just use a single secret key named root key. Though the problems related to wireless networks is been on constant track to be removed but the solutions are not always perfect.

The main two problems that have been faced by the wireless network are security and signal interference. The problem with security can never be solved fully but it can be minimized. Since 1990, many wireless security protocols have been designed and implemented, but none proved to be convincing with the security threats that come every day with new dangers to our systems and information. So, depending on the business needs and requirements it is very much important to address wireless network security more efficiently. Through the last two decades wireless network researchers have come with 3 main Security protocols: WEP, WPA and WPA2 [1]. Wireless Equivalent Privacy) (WEP) was the first default encryption protocol introduced in the first IEEE 802.11 standard, received a great deal of coverage due to various technical failures in the protocol. Wi-Fi protected access (WPA) came with the purpose of solving the problems in the WEP cryptography method.

First WEP, then WPA are used to secure wireless communications were found inadequate due to many proven vulnerabilities so a new protocol was implemented, Wi-Fi protected access 2 (WPA2) protocol. WPA2 also known as IEEE 802.11i standard is an amendment to the 802.11 standard which specifying security mechanisms for wireless networks. Because of the convenience of Wireless LAN (WLAN), it develops quickly. But the security of the WLAN becomes more important at the same time [2]. Compared to wire LAN hacker can break into WLAN more easily because wireless data with electromagnetic wave are transmitted on air. Although WLAN 802.11b protocol provides some security mechanisms, they have some weaknesses and hacker can attack WLAN easily by making use of these weaknesses.

In this paper, we investigate wireless local area networks (WLANs) and security protocols available for WLANs. These existing security protocols have certain vulnerabilities and often hamper network performance as maintain poor trade-off between security and overhead on network performance.

Purpose of the Study

This study discusses the information technology and security metrics used in various wireless LANs. This study identifies specific metrics to compare wireless LANs with respect to a network administrator's requirements: WLAN protocol options, and the respective performance, security configurations, as well as the cost of ownership that is significantly impacted by the depth of interoperability goals.

WLAN characteristics

In this subsection we will discuss the WLAN characteristics that are pertinent to security protocols design.

Roaming: It is the ability to deliver services to wireless stations outside of the basic service area. When a wireless station is roaming, new authentication through the wireless medium must be performed to ensure the new origination of communication and the new session key from unauthorized access and use. In this case it is desirable that the new security mechanisms performed in the new service area should be kept minimal to assure seamless transfer between the areas.

Reduce power consumption: Since the WLANs are intended for portable battery operated wireless stations, low power consumption is a very important consideration. Therefore, the security mechanisms developed should use relatively low complexity cryptographic algorithms. **Limited bandwidth:** The limited ISM frequency band allocated by the FCC and the requirement to use spread spectrum communication limit the data rate. For example in the IEEE 802.11 standard the data rate is up to 2 Mbps [3]. This characteristic will require security protocol design that minimizes the number of messages exchanged over the wireless medium.

Noisy channel: In WLANs the bit error rate is high relatively to wired transmission medium. This characteristic will dictate security protocols that incorporate appropriate provisions for erroneous messages and retransmission procedures.

Wireless Equivalent Privacy (WEP)

WEP is an encryption algorithm developed by an IEEE volunteer group. The aim of WEP algorithm is to provide a secure communication over radio signals between two each end users of a WLAN. WEP uses two key sizes: 40 bit and 104 bit; to be added a 24-bit initialization vector (IV) that is transmitted directly. WEP is a protocol that utilizes RC4 encryption and a 24 bit IV. It began with a 40 bit key that was later expanded to 104 bits. The keys it uses are called Pre-shared Keys (PSK) [4]. The keys are manually entered. WEP adds a checksum of 32 bits called the Integrity Check Value (ICV) to the end of a packet. The authentication method is weak and even helps attackers decipher the key.

Another problem with WEP is that we have to manually configure the key for each wireless device used. This can be problematic if a key is compromised in a large network relying on that key because every device on the network must have their keys changed that creates a logistical in a university or enterprise setting. This discourages organizations from implementing WEP. It also discourages organizations using WEP from ever changing keys. After some years of the implementation of WEP, many flaws like insecure ICV, IV key reuses attack; known plaintext attack, partial known plaintext attack, authentication forging, dictionary attacks, real-time decryption etc were discovered in it. Some of the main weaknesses of WEP are discussed below.

Key Management and Key Size

Key management is not specified in the WEP standard, and therefore is one of its weaknesses, because without interoperable key management, keys will tend to be long-lived and of poor quality. Most wireless networks that use WEP have one single WEP key shared between every node on the network. Access Points (APs) and client stations must be programmed with the same WEP key. Since synchronizing the change of keys is tedious and difficult, keys are seldom changed. In addition, the size of the key---40 bits---has been cited as a weakness of WEP [5]. When the standard was written in 1997, 40 bit keys were considered reasonable for some applications. Since the goal was to protect against "casual eavesdropping" it seemed sufficient at the time.

The Initialization Vector (IV) is too small

WEP's IV size of 24 bits provides for 16,777,216 different RC4 cipher streams for a given WEP key, for any key size. Remember that the RC4 cipher stream is XOR-ed with the original packet to give the encrypted packet which is transmitted, and the IV is sent in the clear with each packet. The problem is IV reuse. If the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV, or, can forge packets. This means that you don't need to know the WEP key to decrypt packets if you know what the key stream was used to encrypt that packet [6]. They sound like similar problems, but it's actually much easier to discover the key stream than it is to discover the WEP key. Since there are only 16 million IV values, how the IV is chosen makes a big difference in the attacks based on IV. Unfortunately, WEP doesn't specify how the IV is chosen or how often the IV is changed. Some implementations start the IV at zero and increase it incrementally for each packet, rolling over back to zero after 16 million packets have been sent. Some implementations choose IVs randomly.

The Integrity Check Value (ICV) algorithm is not appropriate

The WEP ICV is based on CRC-32, an algorithm for detecting noise and common errors in transmission. CRC-32 is an excellent checksum for detecting errors, but an awful choice for a cryptographic hash. Better-designed encryption systems use algorithms such as MD5 or SHA-1 for their ICVs [7]. The CRC-32 ICV is a linear function of the message meaning that an attacker can modify an encrypted message and easily fix the ICV so the message appears authentic. Being able to modify encrypted packets provides for a nearly limitless number of very simple attacks. The biggest problem with IV and ICV-based attacks is they are independent of key size, meaning that even huge keys all look the same. The attack takes the same amount of effort.

WEP’s use of RC4 is weak

RC4 in its implementation in WEP has been found to have weak keys. Having a weak key means that there is more correlation between the key and the output than there should be for good security. Determining which packets were encrypted with weak keys is easy because the first three bytes of the key are taken from the IV that is sent unencrypted in each packet. This weakness can be exploited by a passive attack. All the attacker needs to do is be within a hundred feet or so of the AP. WPA Wi-Fi Protected Access (WPA), the successor of WEP, is a security protocol that implements majority of IEEE 802.11i standard. WPA was created by the Wi-Fi Alliance as an interim solution to replace WEP before 802.11i standard was ready. WPA vastly improves WEP’s encrypting process and adds a concrete user authentication mechanism. In WPA users can be either authenticated through an IEEE 802.1X. Authenticate Server (often a RADIUS server) or through an access point with a passphrase in Pre-shared key (PSK) mode.

WPA also provides software upgrades to accomplish interoperability with the older network cards and access points. WPA uses the RC4 stream cipher with the 128-bit keys and 48-bit IV in encryption. RC4 is still used, because it’s compatible with the old hardware [8]. In addition, WPA introduces a new key security protocol, Temporal Key Integrity Protocol (TKIP), which dynamically changes the keys during the session. As a result the repetition of the same traffic keys is prevented. For this TKIP uses a packet sequencing discipline and a two-phase per-packet key mixing function. Packet sequencing discipline means that every encryption key is associated with a sequence number. This effectively prevents replay attacks. The per packet mixing function takes this sequence number along with the base WPA key and the transmitter MAC address as inputs, and outputs a new per packet WPA key. This new WPA key is then used along with the IV to generate the key stream

802.11i (WPA2)

This is essentially the certified name for IEEE 802.11i by the Wi-Fi Alliance, and can be thought of as synonymous with IEEE 802.11i. The main difference between WPA and WPA2 is the requirement of CCMP encryption with WPA2. Like WPA, WPA2 is also available in Personal and Enterprise modes. WPA2 allows an easy transition from WPA mode by using WPA/WPA2 mixed mode, so networked computers can use either WPA or WPA2. It doesn't employ RC4 like WEP or WPA; it uses Counter Mode with CBC-MAC Protocol (CCMP) to encrypt network traffic. CCMP employs Advanced Encryption Standard (AES) as encryption algorithm [9]. 802.11i is backwards compatible with WPA but not with WEP.

Thus WPA2 is most secure among existing security protocols but has few complexities related to its encryption overheads. High power consumption is still posing problems in WPA2. The overhead associated with WPA2 is increased drastically due to this strong AES mechanism in this protocol. Like WEP, WPA2 also uses only one algorithm and one key to encrypt and decrypt the all the packets. Thus if the mechanism is compromised once, it cannot be maintained back. Thus it is also not maintainable. Moreover, when the network is large that is we are having large number of nodes in the network, overhead on network performance associated due to WPA2 will be very high.

Weaknesses of WPA/WPA2

Although WPA/WPA2 security schemes are strong, attacks against them have already been implemented. These attacks are based on user’s tendency to choose weak passwords that are easy to guess. Cowpatty is a tool that goes through all possible key combinations (brute force) starting with the easiest choices. With this strategy an easy password may be cracked. The root cause for this problem lies in the lack of usability [10]. In other words, when setting up a wireless network, users still have to enter the keys manually, which is time consuming and can be too challenging for the beginners. Therefore the WPA/WPA2 security scheme still needs to be developed.

Comparing WPA with WEP

WPA and WEP both use RC4 stream cipher for encryption. However, instead of the standard WEP’s combination of 24- bit IV and 40/104-bit key, WPA employs a 48-bit IV together with a 128-bit key. WEP’s inadequate security resulted from IV collisions and altered packets. In WPA, these problems have been eliminated with a combination of Temporal Key Integrity Protocol (TKIP), Message Integrity check (MIC) and extended IV space. TKIP’s key hierarchy exchanges WEP’s single static key for roughly 500 trillion possible keys that can be used to encrypt a packet. Combined with a 48-bit IV, TKIP effectively makes the attacks based on recovering the key infeasible [11]. MIC and its cryptographic algorithm, "Michael", put a stop to the packet forgery that was possible in WEP due to CRC’s linearity.

The 802.1X/EAP framework and PSK-mode provides WPA a concrete user authentication mechanism, which was largely missing in WEP. As mentioned earlier, in WEP, the user could be authenticated with the Shared-Key Authentication mechanism, an optional feature that involves the use of challenges. This scheme relies on the use of the same pre-shared WEP key that was used in encryption, and therefore was proven to be a security risk. In WPA the encryption and the authentication are separated [12]. After authenticating to the 802.11x server/AP with credentials/passphrase the keys are distributed to the user automatically.

The relationship between WPA2, WPA and WEP is presented in the table below

	WEP	**WPA**	**WPA2**
Encryption cipher.	RC4	RC4	AES
Key sizes	40/104 bit	128 bit	128 bit

IV size	24 bit	48 bit	48 bit
Per-packet key	Key + IV	TKIP mix.fc.	CCM
Data integrity	CRC-32	Michael	CCM
Replay detection	None	IV seq.	IV seq.
Key management	None	802.1X	802.1X

Experiment

The objective of this section is to determine the overhead associated with IEEE 802.11 security protocols. More security is required on wireless networks to ensure reliability and data integrity. Applications associated with the use of wireless networks are continually expanding, and they could be impacted by slow response times or reduced throughput. Although not all of these issues are directly addressed in this paper, it should help to develop the need for a thorough understanding of the effects that security could cause on various types of network performance. As such the paper intends to provide general overviews of the current security protocols in use today and expose the vulnerability of wireless local area network; and how they compare to one another with respect to response time, latency, and throughput.

To conduct these experiments used BACKTRACK and aircrack-ng. Aircrack-ng will read in unique IVs from all the capture files and then perform a statistical attack on those IVs. It involves the physical layer implementations of 802.11b and 802.11g with available MAC layer configuration and possible theoretical data rates specified by IEEE. The security protocols that we have implemented in this experiment include WEP, WPA and WPA2.

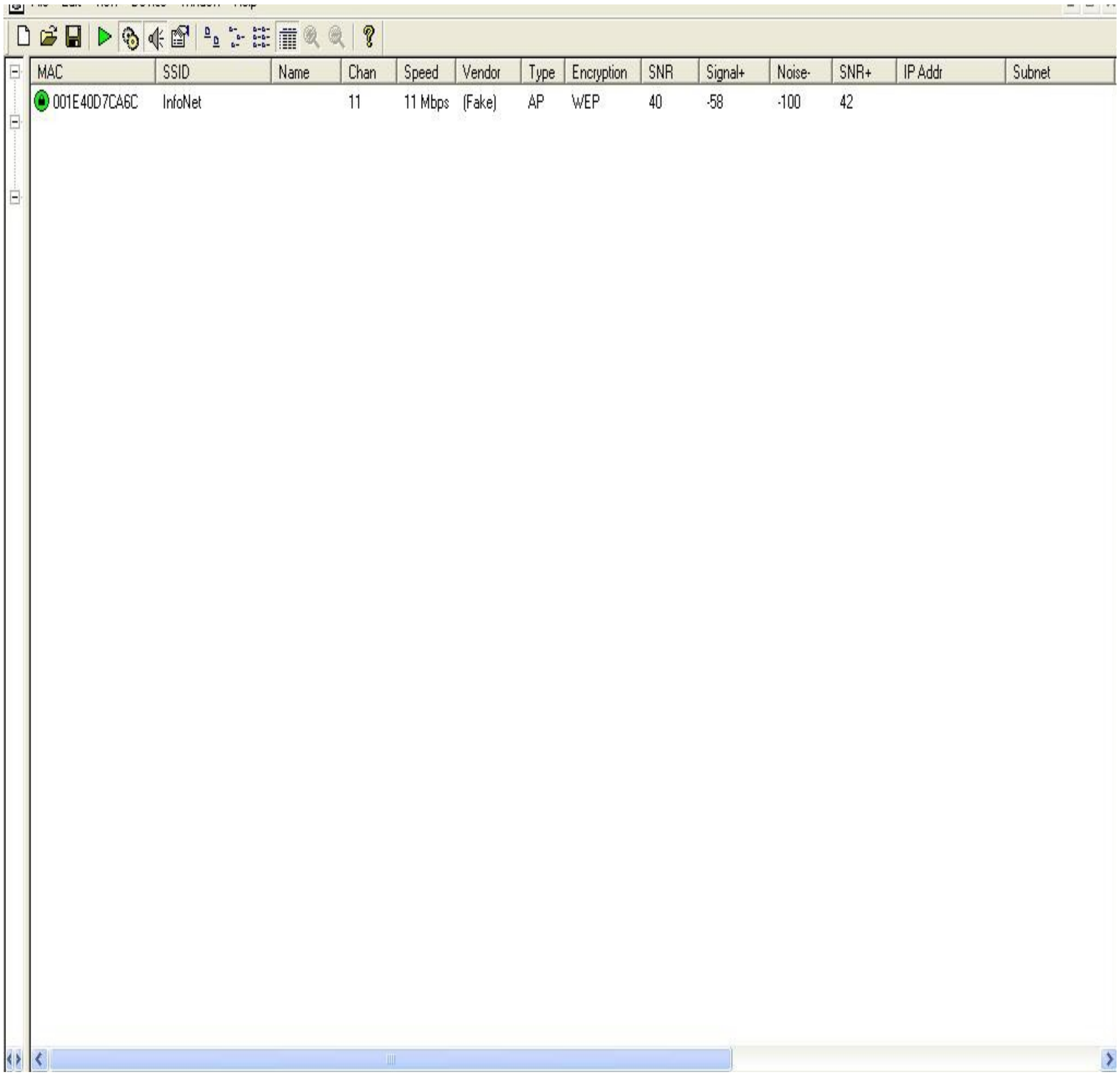
Parameters

The performance measurements of our simulation are total simulation time, throughput, packet delivery fraction and average end-end packet delivery fraction. We have also measured Total Simulation Time Distribution and throughput for 20 and 50 nodes at different data rates.

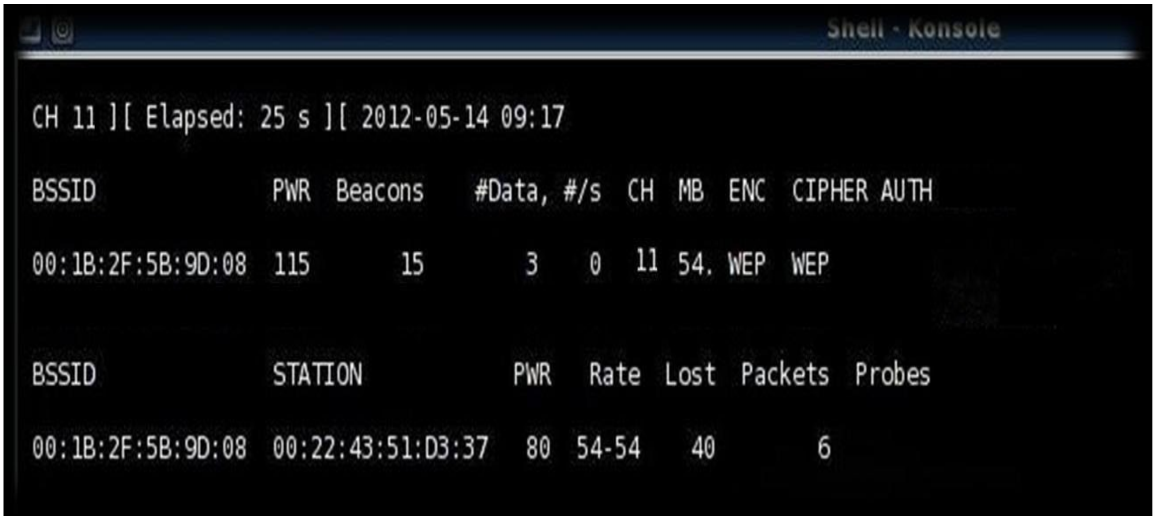
Results

In our experiment, we have evaluated several configurations for 802.11b and 802.11g networks and obtained several performance values. Here, we are highlighting the comparison between WEP, WPA and the most secure security mechanism WPA2 in WLAN on the basis of various network performance metrics. The following figures show some of the interesting results of our evaluation using aircrack-ng and Backtrack.

WEP Result

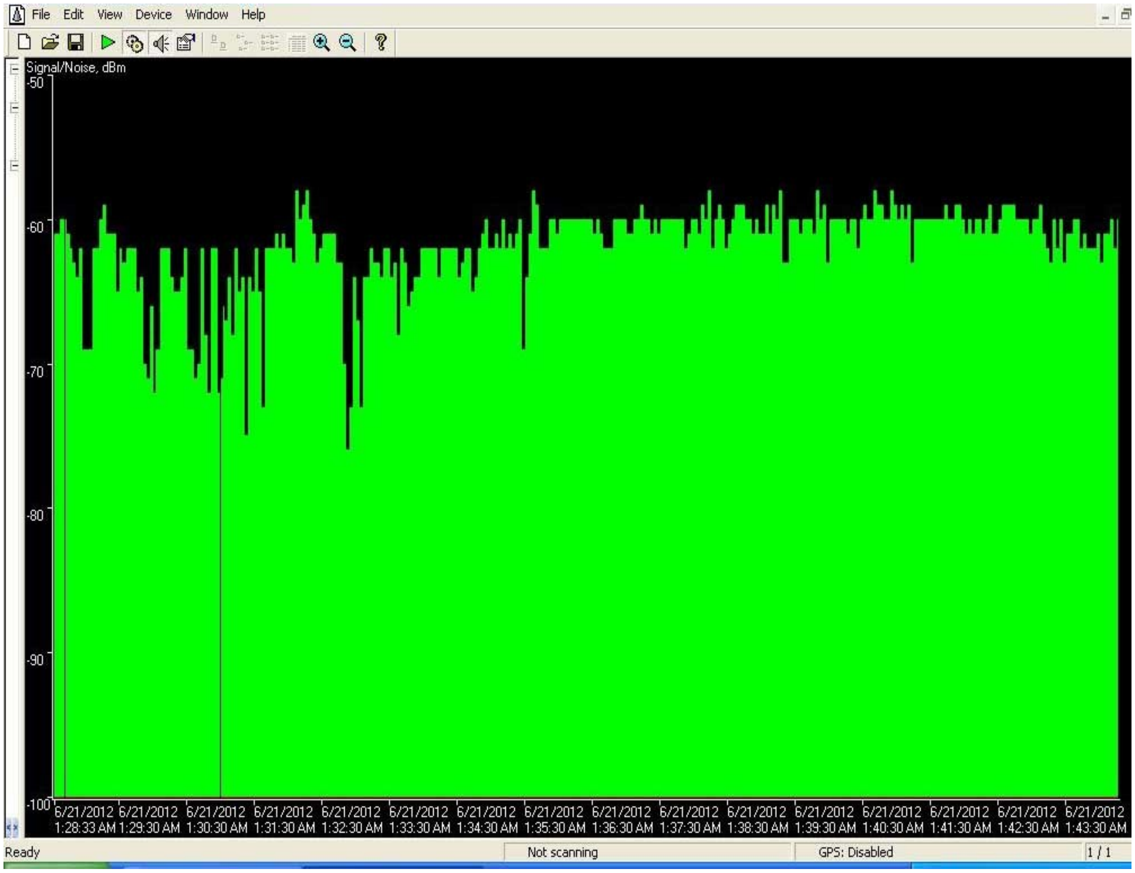


MAC	SSID	Name	Chan	Speed	Vendor	Type	Encryption	SNR	Signal+	Noise-	SNR+	IP Addr	Subnet
● 001E40D7CA6C	InfoNet		11	11 Mbps	(Fake)	AP	WEP	40	-58	-100	42		

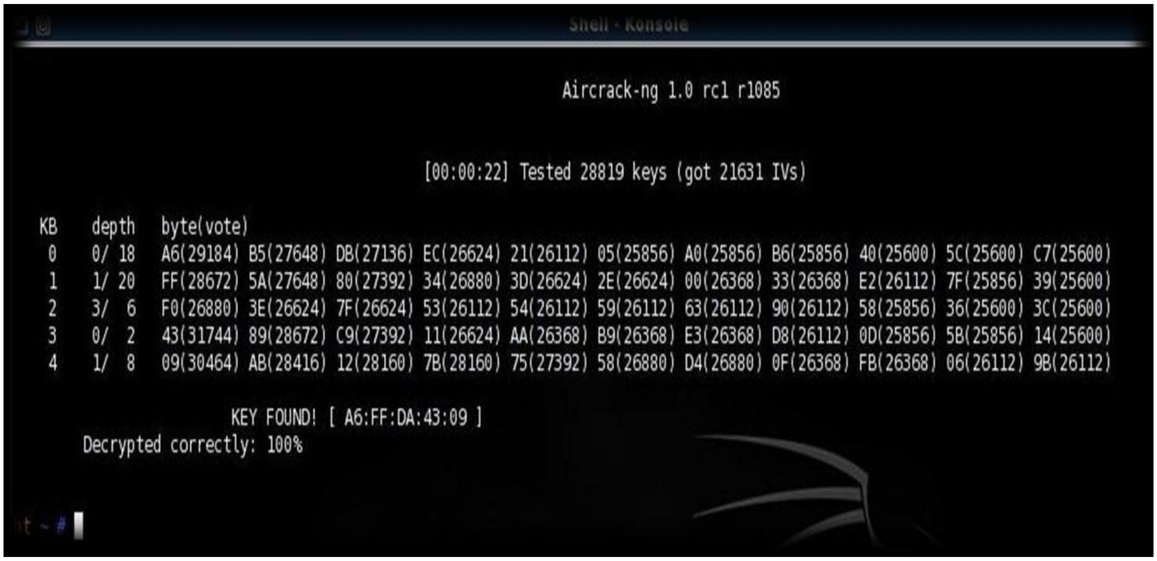


```
CH 11 ][ Elapsed: 25 s ][ 2012-05-14 09:17

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH

00:1B:2F:5B:9D:08  115       15        3    0  11 54. WEP  WEP

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:1B:2F:5B:9D:08  00:22:43:51:D3:37   80  54-54    40        6
```

Here shows the detail of WEP description using BACKTRACK. In this the channel shown is 11. But it is not necessary that the channel will always be 11 for this. If we disconnect the modem and connect it aging then we can get other channels like 12, 44, 53, etc also.



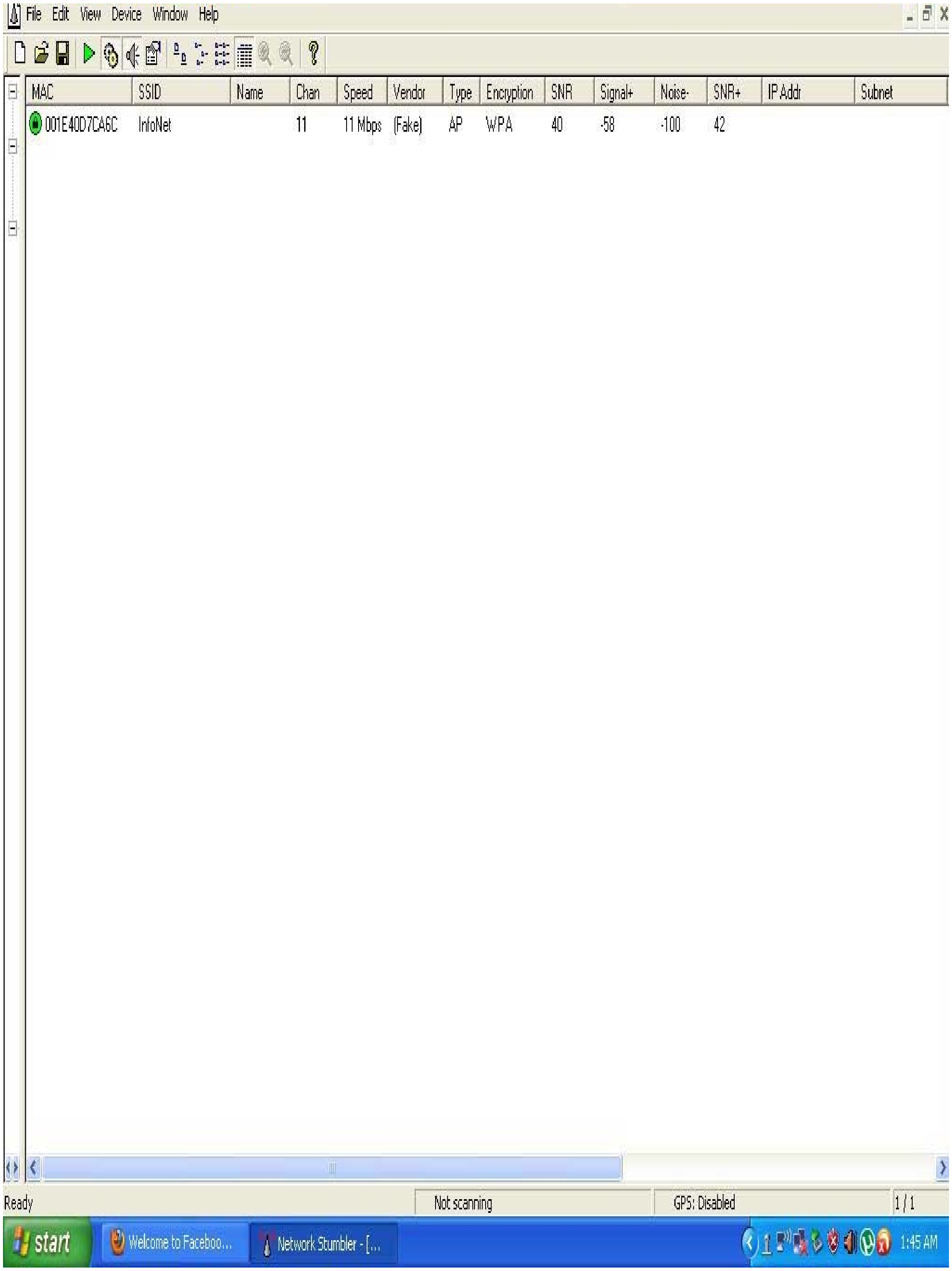
In the above graph shown, we can see that after the two attacks the graph is fully constant which means that it is not a better security.



```
                                   Aircrack-ng 1.0 rc1 r1085


                        [00:00:22] Tested 28819 keys (got 21631 IVs)

 KB    depth   byte(vote)
  0    0/ 18   A6(29184) B5(27648) DB(27136) EC(26624) 21(26112) 05(25856) A0(25856) B6(25856) 40(25600) 5C(25600) C7(25600)
  1    1/ 20   FF(28672) 5A(27648) 80(27392) 34(26880) 3D(26624) 2E(26624) 00(26368) 33(26368) E2(26112) 7F(25856) 39(25600)
  2    3/  6   F0(26880) 3E(26624) 7F(26624) 53(26112) 54(26112) 59(26112) 63(26112) 90(26112) 58(25856) 36(25600) 3C(25600)
  3    0/  2   43(31744) 89(28672) C9(27392) 11(26624) AA(26368) B9(26368) E3(26368) D8(26112) 0D(25856) 5B(25856) 14(25600)
  4    1/  8   09(30464) AB(28416) 12(28160) 7B(28160) 75(27392) 58(26880) D4(26880) 0F(26368) FB(26368) 06(26112) 9B(26112)

                   KEY FOUND! [ A6:FF:DA:43:09 ]
     Decrypted correctly: 100%


t ~ #
```

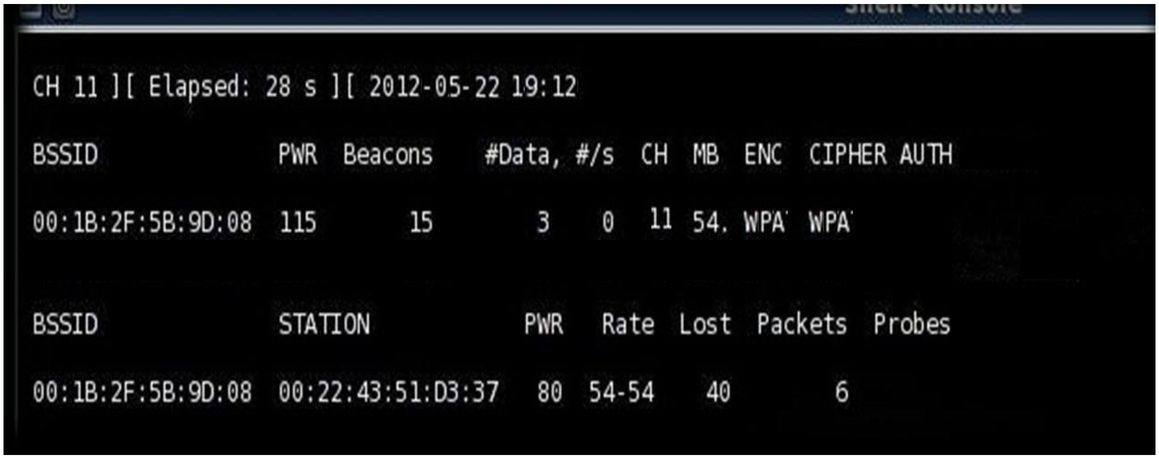
As demonstrated above, WEP cracking has become increasingly easier over the years, in past it may required hundreds, thousands packets or days of capturing data to crack the WEP but now a days it can be accomplished within few minutes approximately 20k data packets. WEP attack can be minimized or harder by using longer IVs size like 48 bit long IVs rather than 24-bit long IVs and this security is cracked in 22 seconds.

WPA Result



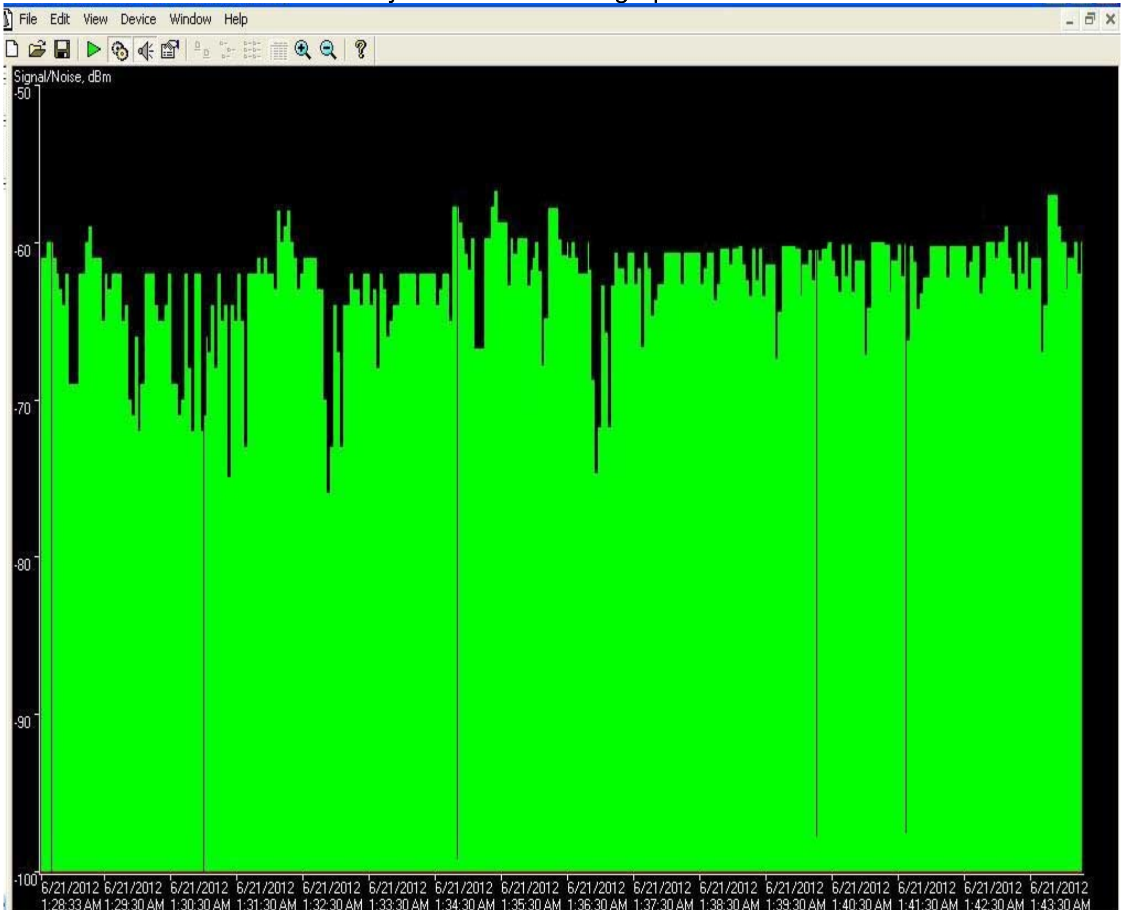
MAC	SSID	Name	Chan	Speed	Vendor	Type	Encryption	SNR	Signal+	Noise-	SNR+	IP Addr	Subnet
001E40D7CA6C	InfoNet		11	11 Mbps	(Fake)	AP	WPA	40	-58	-100	42		

Ready | Not scanning | GPS: Disabled | 1 / 1

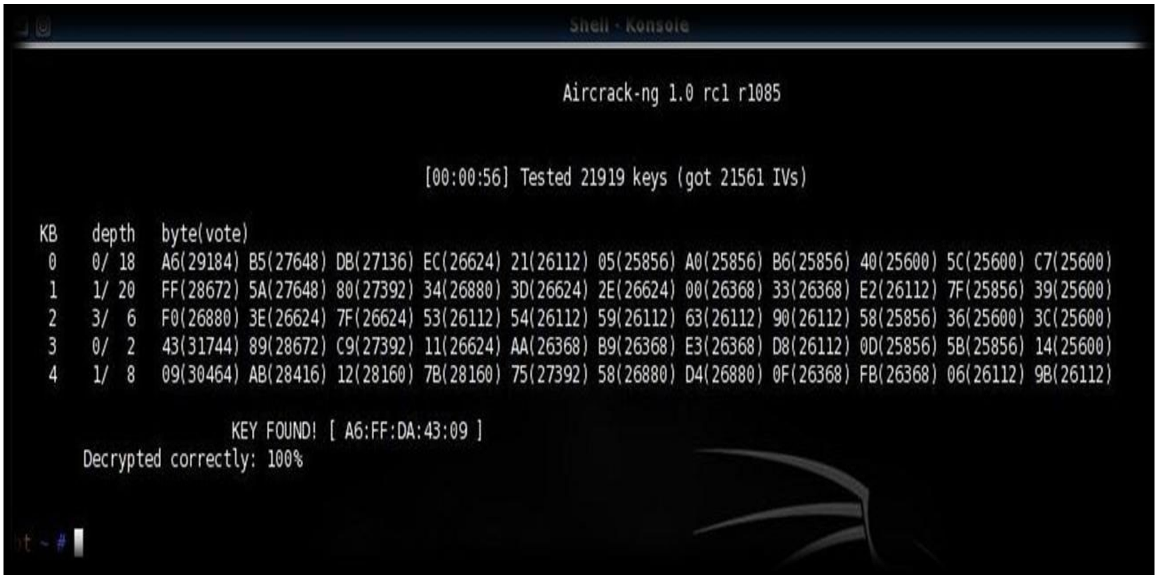


```
CH 11 ][ Elapsed: 28 s ][ 2012-05-22 19:12

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH

00:1B:2F:5B:9D:08  115       15        3    0  11  54. WPA  WPA

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:1B:2F:5B:9D:08  00:22:43:51:D3:37   80  54-54    40        6
```

Here the channel of WPA security shown is 11. The graph of WPA is shown below:



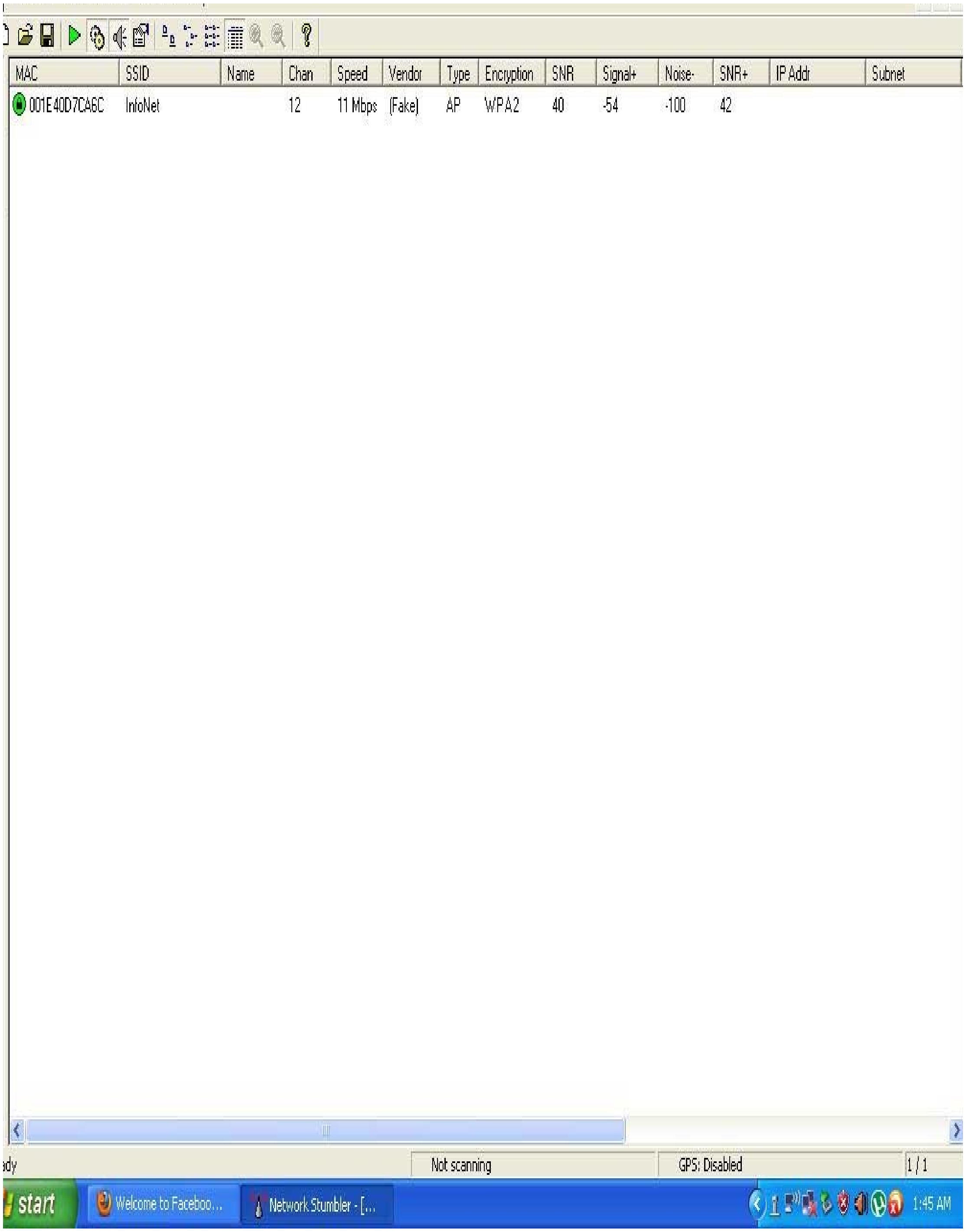
In this graph, we conclude that after applying more than two attacks, it also becomes constant for sometime.



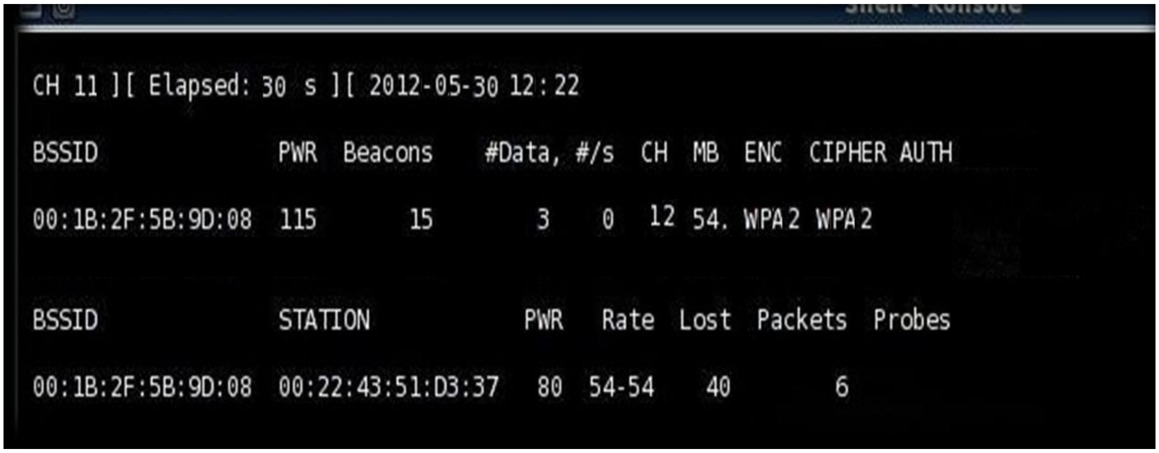
```
                                 Aircrack-ng 1.0 rc1 r1085


                         [00:00:56] Tested 21919 keys (got 21561 IVs)

   KB    depth   byte(vote)
    0    0/ 18   A6(29184) B5(27648) DB(27136) EC(26624) 21(26112) 05(25856) A0(25856) B6(25856) 40(25600) 5C(25600) C7(25600)
    1    1/ 20   FF(28672) 5A(27648) 80(27392) 34(26880) 3D(26624) 2E(26624) 00(26368) 33(26368) E2(26112) 7F(25856) 39(25600)
    2    3/  6   F0(26880) 3E(26624) 7F(26624) 53(26112) 54(26112) 59(26112) 63(26112) 90(26112) 58(25856) 36(25600) 3C(25600)
    3    0/  2   43(31744) 89(28672) C9(27392) 11(26624) AA(26368) B9(26368) E3(26368) D8(26112) 0D(25856) 5B(25856) 14(25600)
    4    1/  8   09(30464) AB(28416) 12(28160) 7B(28160) 75(27392) 58(26880) D4(26880) 0F(26368) FB(26368) 06(26112) 9B(26112)

                      KEY FOUND! [ A6:FF:DA:43:09 ]
        Decrypted correctly: 100%


 t ~ #
```

This shows that using the WPA pre-shared key is not fully secure. Although this attack does work 100% but if end user uses the common world phrase it can be easily break. By using Back Track3 this security is cracked in 56 seconds. So Encryption of WPA2-PSK is more secure and strong than WPA-PSK because WPA got cracked after sometime and WPA2-PSK uses the long phrases than WPA.

WPA2 Result

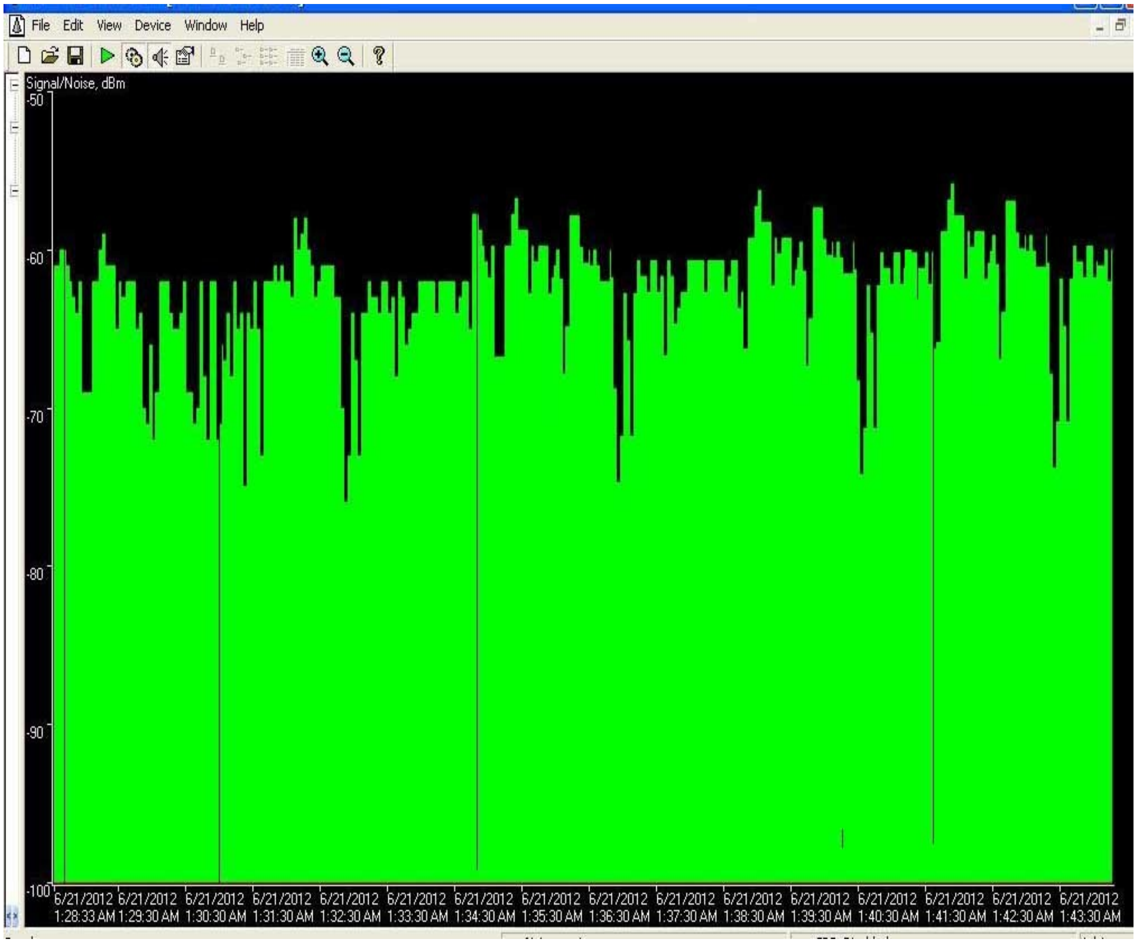


MAC	SSID	Name	Chan	Speed	Vendor	Type	Encryption	SNR	Signal+	Noise-	SNR+	IP Addr	Subnet
001E40D7CA6C	InfoNet		12	11 Mbps	(Fake)	AP	WPA2	40	-54	-100	42		

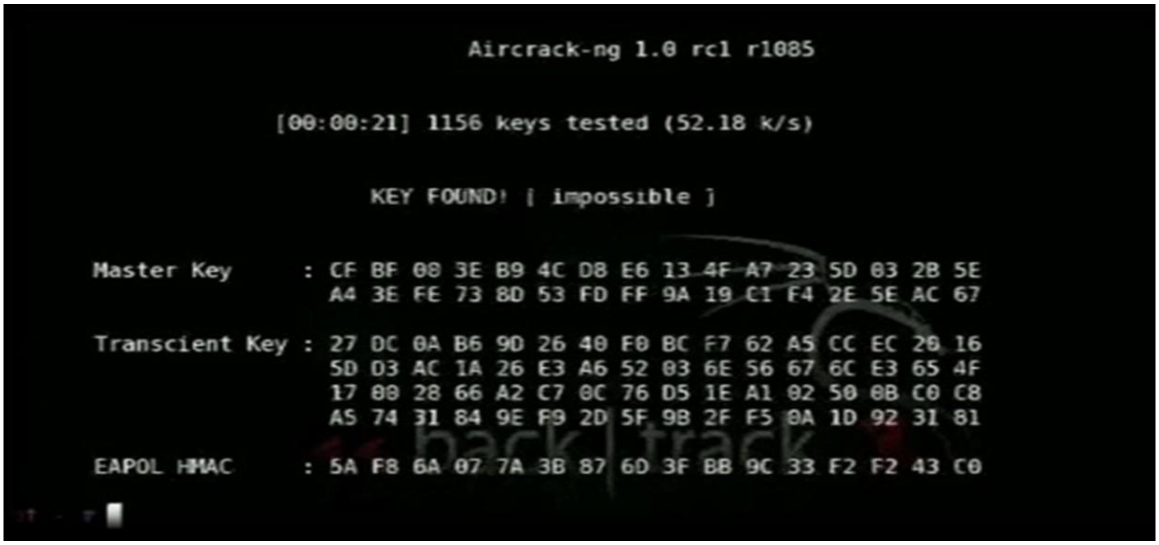


```
CH 11 ][ Elapsed: 30 s ][ 2012-05-30 12:22

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH

00:1B:2F:5B:9D:08  115       15        3    0  12 54. WPA2 WPA2


BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:1B:2F:5B:9D:08  00:22:43:51:D3:37   80  54-54    40       6
```

Here the channel shown is 12 and the encryption type is WPA2. The graph of WPA2 is shown below:



This graph shows that when we apply as many attacks this security cannot become constant which means that it is most secure as compared to other securities.



```
                          Aircrack-ng 1.0 rc1 r1085

                 [00:00:21] 1156 keys tested (52.18 k/s)

                       KEY FOUND! [ impossible ]

  Master Key     : CF BF 08 3E B9 4C D8 E6 13 4F A7 23 5D 03 2B 5E
                   A4 3E FE 73 8D 53 FD FF 9A 19 C1 F4 2E 5E AC 67

  Transcient Key : 27 DC 0A B6 9D 26 40 F0 BC F7 62 A5 CC EC 20 16
                   5D D3 AC 1A 26 E3 A6 52 03 6E 56 67 6C E3 65 4F
                   17 00 28 66 A2 C7 0C 76 D5 1E A1 02 50 0B C0 C8
                   A5 74 31 84 9E F9 2D 5F 9B 2F F5 0A 1D 92 31 81

  EAPOL HMAC     : 5A F8 6A 07 7A 3B 87 6D 3F BB 9C 33 F2 F2 43 C0
```

This section shows that using the WPA2 pre-shared key is fully secure. Although this attack does work 100% as by using Back Track3 this security is not cracked. So Encryption of WPA2-PSK is more secure and strong because it uses the long phrases.

Conclusion

In this paper, we have analyzed the performance of wireless local area networks (WLANs) and security strength of standard security protocols available in WLANs and their overhead as performance concern. These available security mechanisms are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and WPA2. Each existing security protocol in WLAN has various vulnerabilities as highlighted earlier. Among these existing security protocols in WLANs, WPA2 is the most secure security protocol but trade-off between security and overhead associated with it is not good.

References

[1] IEEE Computer Society. *Wired Equivalent Privacy*, 1999.

[2] Wi-Fi Alliance. *Wi-Fi Protected Access*, 2003.

[3] B. Schneier, *Applied Cryptography*: Protocols, Algorithms and Source Code in C. New York: Wiley, 1996, pp. 397–398.

[4] L. M. S. C. of the IEEE Computer Society. *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*. IEEE Standard 802.11, 1999 Edition, 1999.

[5] America Online and the National Cyber Security Alliance, *AOL/NCSA Online Safety Study* conducted in December 2005.

[6] William A. Arbaugh *An Inductive Chosen Plaintext Attack against WEP/WEP2*, 2001.

[7] "*Understanding the updated WPA and WPA2 standards*".ZDNet Blogs. Posted by George Ou. June 2 2005. <http://blogs.zdnet.com/Ou/?p=67>

[8] "*Deploying Wi-Fi Protected Access* (WPAtm) and WPA2tm in the Enterprise." Wi-Fi Alliance, Feb. 27 2005<http://www.wifi.org/files/uploaded_files/wp_9_WPAWPA2% 20Implementation_2-27-05.pdf>

[9] WPA: *A Key Step Forward in Enterprise-class Wireless* LAN (WLAN) Security, Jon A. LaRosa, Meeting House data communications, 2003

[10] *Wi-Fi Protected Access*: Strong, standards-based, interoperable security for today's Wi-Fi networks, Wi-Fi Alliance, 2003 www.weca.net5

[11] 802.11 *Security Series Part II: The Temporal Key Integrity Protocol* (TKIP), Jesse Walker, Intel Corporation, 2002

[12] *The evolution of wireless security in 802.11 networks*: WEP, WPA and 802.11 standards Stanley Wong GSEC Practical v1.4b, 2003